MATH 370 Lecture 4

Recap from previous lecture:

Defn: Let G_1, G_2 be two groups. A map $\varphi: G_1 \to G_2$ is called group homomorphism if $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G_1$.

Group homomorphisms give rise to two subgroups

1) $\ker \varphi \subseteq G_1$

$\| $

$\{ g \in G_1 \mid \varphi(g) = e \}$

2) $\operatorname{Im} \varphi \subseteq G_2$

$\| $

$\{ \varphi(g) \mid g \in G_1 \}$

Examples: 1) $\varepsilon : S_n \longrightarrow \{\pm 1\}$

$\downarrow$

Signature of a permutation

$\ker \varepsilon = A_n \qquad \operatorname{Im} \varepsilon = \{\pm 1\}$

2) $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R} - \{0\}$

$\ker \det = SL_n(\mathbb{R})$

$\operatorname{Im} \det = \mathbb{R} - \{0\}$

3) $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R} - \{0\}, \times)$

$r \longmapsto e^r$

$\ker \exp = \{0\}$

$\operatorname{Im} \exp = \{ r \in \mathbb{R} - \{0\} \mid r > 0 \}$

ISOMORPHISMS

Let G_1, G_2 be two groups. Let

$\varphi: G_1 \to G_2$ be a group homomorphism

Defn: We say that φ is isomorphism if φ is bijective.

Aside: This notion of "algebraic isomorphism" is different from "topological isomorphism" where a set theoretic inverse need not be continuous. So a homeomorphism is a continuous map that has a continuous inverse.

Lemma: φ is group isomorphism

$\iff \ker\varphi = \{e\}$ & $\operatorname{Im}\varphi = G_2$.

Pf: $\Rightarrow$ follows from definition

$\Leftarrow$ If $\ker\varphi = \{e\}$, then φ is injective

because if $\varphi(g_1) = \varphi(g_2)$

$\Rightarrow \varphi(g_1)\,\varphi(g_2)^{-1} = e$

$\Rightarrow \varphi(g_1)\,\varphi(g_2^{-1}) = e$

$\Rightarrow \varphi(g_1 g_2^{-1}) = e$

$\Rightarrow g_1 g_2^{-1} \in \ker\varphi$ so $g_1 g_2^{-1} = e$

$\Rightarrow g_1 = g_2$.

Proof now follows.

Examples: 1) Let G be any group.

$$\varphi : G \to G$$
$$g \mapsto g$$

Terminology: An isomorphism from a group to itself is called automorphism.

2) $$\varphi : G \to G$$
$$g \longmapsto g^{-1}$$

$\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} \neq \varphi(g)\varphi(h)$

φ is not a homomorphism but we can make it into one!

Define $G^{op} = (G, op)$

$g_1 \, op \, g_2 = g_2 g_1$

($g_2 g_1$: original group operation on G)

$\varphi : G \longrightarrow G^{op}$

$g \longmapsto g^{-1}$

$\varphi(gh) = (gh)^{-1} = h^{-1} g^{-1}$

$= \varphi(g) \, op \, \varphi(h)$

φ is group hom.

$\ker \varphi = \{e\}$

$\operatorname{im} \varphi = G^{op}$

$\Rightarrow \varphi$ is isomorphism.

3) Conjugation — Fix $g \in G$

$\varphi_g : G \to G$

$h \longmapsto ghg^{-1}$

$$\varphi_g(h_1h_2) = g h_1 h_2 g^{-1}$$

$$\varphi_g(h_1)\,\varphi_g(h_2) = (g h_1 g^{-1})(g h_2 g^{-1})$$

$$= g h_1 h_2 g^{-1}$$

So, φ_g is a group homomorphism.

$$\ker \varphi_g = \{ h \in G \mid ghg^{-1} = e \}$$

$$= \{ h \in G \mid gh = g \}$$

$$= \{ h \in G \mid h = e \}$$

$$= \{e\}$$

For any $h \in G$

$$\varphi_g(g^{-1}hg) = g(g^{-1}hg)g^{-1}$$

$$= h$$

So, $\text{im}\,\varphi_g = G$

Hence, φ_g is an automorphism.

RELATIONS

Let S be a set.

Defn: A relation R is a subset of $S \times S$.

Example: Let $f : S \to S$ be a function.

Then $\{(s, f(s)) \mid s \in S\} \subseteq S \times S$ is a relation.

Defn: (1) (Reflexive) If $(s,s) \in R \quad \forall s \in S$.

(2) (Symmetric) $(s,t) \in R \Rightarrow (t,s) \in R$

(3) (Transitive) (a,b) & $(b,c) \in R$

$\Rightarrow (a,c) \in R$

Alternate notation If $(a,b) \in R$, we will say that $a \sim b$ or $a \sim_R b$ (if one wants to emphasize the relation)

Qn: Let $S = \mathbb{Z}$. Define a relation R on $\mathbb{Z}$ as follows

$$a \sim b \iff a | b$$

(1) Is it reflexive?

(2) Is it symmetric?

(3) Is it transitive?

Qn: Let $S = \mathbb{Z}$. Define a relation R on $\mathbb{Z}$ as follows.

$$a \sim b \iff a < b$$

(1) Is R reflexive?

(2) Is R symmetric?

(3) Is R transitive?

EQUIVALENCE RELATION

Defn: A relation R which is reflexive, Symmetric and transitive.

Example of integers ($\mathbb{Z}$)

Euclid's division lemma: For $b \in \mathbb{Z}$, $m \in \mathbb{Z}$ $(m \neq 0)$ there exists unique integers q and r Such that

quotient

1. $b = mq + r$ — remainder
2. $r \in \{0, 1, 2, \ldots |m| - 1\}$

Define a relation R on $\mathbb{Z}$ as follows. Fix $m \in \mathbb{N}$.

$a \sim b \iff$ a and b leave same remainder when divided by m

(also denoted as $a \equiv b \pmod m$)

(1) R is reflexive

(2) R is symmetric

(3) R is transitive

So R is an equivalence relation.

This creates a "partition" on $\mathbb{Z}$.

$m = 2$ All even integers are related to each other

All odd ——————.

$\mathbb{Z}$ = {odd integers} $\sqcup$ {Even integers}

↓ Denote as

$[1] \sqcup [0]$

$[1]$ ↳ Class of 1 $[0]$ ↳ Class of 0

$m = 3$ $\mathbb{Z} = \{3q\} \sqcup \{3q+1\} \sqcup \{3q+2\}$

$= [0] \sqcup [1] \sqcup [2]$

In general, we have

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [m-1]$$

Define $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], [2], \ldots [m-1]\}$

We can define addition on $\mathbb{Z}/m\mathbb{Z}$ as follows.

$$[r] + [s] = [r+s]$$

Qn: Why is this well-defined?

This defines a binary operation on $\mathbb{Z}/m\mathbb{Z}$.

Is $(\mathbb{Z}/m\mathbb{Z}, +)$ a group?

Similarly we can define multiplication on $\mathbb{Z}/m\mathbb{Z}$

$$[r] \cdot [s] = [rs]$$

Is $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ a group?

In general, equivalence relation create a partition of S and Conversely a partition of S defines an equivalence relation.

$$\{\text{Equivalence relation}\} \longleftrightarrow \{\text{Partitions}\}$$

Set S relation R on S

Pick $s_0 \in S$, $[s_0] = \{t \in S \mid t \sim s_0\}$

If $[s_0] = S$, then we are done, otherwise

Pick $s_1 \notin [s_0]$ and repeat this

Ultimately

$$S = [s_0] \sqcup [s_1] \sqcup \cdots$$

This partition need not be finite.

Conversely if $S = S_0 \sqcup S_1 \sqcup \cdots \quad S_i \subseteq S$

Define $\sim$: $a \sim b \iff a$ & b lie in same S_i